FPKIPA
Federal Public Key Infrastructure Policy Authority

FEDERAL PKI POLICY AUTHORITY

July 10, 2012 MEETING MINUTES

USPS Headquarters
475 L'Enfant Plaza, SW
Conference Room: 4841
Washington, DC
9:30 a.m. – 12:00 a.m. EST

9:30	**Welcome, Opening Remarks & Introductions**	**Deb Gallagher, Chair**
9:35	**Discuss / Vote on June 2012 FPKIPA Minutes**	**Jeff Jarboe**
9:45	**Criticality of FPKI Availability - Update**	**Toby Slusher**
10:00	**FPKI Management Authority (FPKIMA) Report**	**Darlene Gore**
10:30	**FPKI Certificate Policy Working Group (CPWG) Report** 1. EKUs and Technical Constraints 2. Discussion: Delegation of Device Sponsor Responsibilities Change Proposal (Common CP) 3. Discussion: Common Root CA Offline Operation 4. Other Updates	**Charles Froehlich**
11:00	**SHA-1 Transition Status**	**SHA-1 Affiliates**
11:10	**VA Status Update**	**John Hancock / Eric Jurasas**
11:20	**FPKIPA Chair Update**	**Deb Gallagher**
11:30	**Other Agenda Items** ○ *ICAM Update* ○ *If you cannot attend, please designate a proxy* ○ *Next FPKIPA meeting, August 14, 2012*	**Deb Gallagher**
12:00	**Adjourn Meeting**	**Deb Gallagher**

A. ATTENDANCE LIST

a. Voting Members

Organization	Name	T – Telephone P – In Person A – Absent
Department of Defense (DOD)	Mitchell, Debbie	T
Department of Energy (DOE)	Thomas, Michele	T
Department of Health & Human Services (HHS)	Slusher, Toby	T
Department of Homeland Security (DHS)	Miller, Tanyette (Proxy for Don Hagerling)	T
Department of Justice (DOJ)	Morrison, Scott	P
Department of State (State)	Steve Gregory	P
Department of Treasury (Treasury)	Wood, Dan	A
Drug Enforcement Administration (DEA CSOS)	Briggs, Sherrod (Proxy for Chris Jewell)	A
Government Printing Office (GPO)	Hannan, John	A
General Services Administration (GSA)	Gallagher, Deb	P
National Aeronautics & Space Administration (NASA)	Wyatt, Terry	T
Nuclear Regulatory Commission (NRC)	Sulser, David	P
Social Security Administration (SSA)	Mitchell, Eric	T
United States Postal Service (USPS)	Stepongzi, Mark	P
United States Patent & Trademark Office (USPTO)	Lindsey, Dan	T
Veterans Administration (VA)	Jurasas, Eric	A

b. Observers

Organization	Name	T – Telephone P – In Person A – Absent
Safer Institute	Boley, Ken	P
FPKIMA Technical Liaison (Contractor, Protiviti)	Brown, Wendy	P
DoS (Contractor, ManTech)	Froehlich, Charles	P
FPKIPA (Contractor, Protiviti)	Jarboe, Jeff	P
FPKIPA (Contractor, Protiviti)	Silver, Dave	T
CertiPath	Spencer, Judy	P
ExoStar	Baker, George	T
Entrust	Schoen, Isadore	T
GSA FAS	Gore, Darlene	T
DHA (Contractor)	Shomo, Larry	T
CertiPath	Spencer, Judy	P
SAFE BioPharma	Wilson, Gary	T
CertiPath	Barry, Jeff	T
KPMG	Faut, Nathan	P
FPKIPA (Contractor, Protiviti)	Palmer, Kathryn	T

B. MEETING ACTIVITY

Welcome, Opening Remarks & Introductions, Deb Gallagher

The Federal Public Key Infrastructure Policy Authority (FPKIPA) met at USPS Headquarters located at 475 L'Enfant Plaza SW, Washington, DC. Ms. Deb Gallagher, Chair, called the meeting to order at 9:33 a.m. EST. Those present, both in person and via teleconference, introduced themselves.

Discuss / Vote on June 12, 2012 FPKIPA Minutes, Jeff Jarboe

Due to time constraints, there was a vote by acclamation to approve the June 12, 2012 FPKIPA minutes. USPS motioned to accept the June 2012 Minutes and DOJ seconded. No objections were raised and the minutes were approved.

Criticality of FPKI Availability - Update, Toby Slusher

Mr. Toby Slusher provided an update on the Criticality of FPKI Tiger Team. There have been some scheduling challenges, but there are two meetings scheduled for Friday, July 13, 2012. One meeting will be in the morning and the other in the afternoon. The main goal of these meetings is to continue with the criticality explanation. Since the group is operating as a tiger team, Mr. Slusher will be setting up a separate distribution list to keep their interim discussions off the FPKIPA list.

Ms. Debbie Mitchell asked about the final objective of the tiger team effort. The main objective is to develop letters to help raise awareness about the criticality and to help justify FPKI funding.

Ms. Mitchell mentioned that it would have been good to have this ready before the July 2012 CIO meeting. However, Mr. Slusher and Ms. Deb Gallagher emphasized that this effort was started before the GSA Cost Recovery Model was briefed to the FPKIPA, and that it is a separate effort. There are additional opportunities to raise awareness of the criticality of the FPKI - not just articulating it in letter form going through the ICAMSC and CIO counsel. Although it would have been helpful at the July 2012 CIO Council, the effort needs to continue.

Ms. Mitchell asked if there needs to be any agency participation. Ms. Gallagher responded that even though people understand the need within DoD for PKI, it’s not true among all agencies. Among agencies, it’s not fully mandated that PKI be used in all areas that would be beneficial. Developing the letters would address and increase awareness of the importance of PKI.

Mr. Larry Shomo asked how this fits into the CIO cost funding model. Ms. Gallagher stated that there were additional meetings about funding models before the BOAC meeting. Both Ms. Gallagher and Ms. Darlene Gore stated that they have received very little feedback from the BOAC. However, the budget examiners for each agency have accepted the tiered approach. Therefore, unless the CIO Council comes up with a different model, the tiered model will be implemented in FY14.

Although neither Ms. Gore nor Ms. Gallagher were at the BOAC meeting, they believe three funding models were presented to the BOAC last month and that there has been no definitive indication as to which model was selected. Suggestions from the community after last month's FPKIPA meeting were used to develop the models: a tiered approach, even distribution of costs, and the one that GSA started with where DoD received the largest cost.

Ms. Michele Thomas asked if what was presented to the BOAC could be sent to the FPKIPA list. Ms. Gore said she will obtain the presentation and send it to Mr. Jeff Jarboe for distribution.

ACTION ITEMS:

1. Ms. Darlene Gore to provide the briefing that was given to the BOAC to Mr. Jeff Jarboe for distribution to the FPKIPA.

FPKI Management Authority FPKIMA) Report, Darlene Gore

The FPKIMA distributed a survey regarding FPKIMA services. A reminder will be sent indicating there is still time to respond. The FPKIMA welcomes multiple responses from a single agency.

An update on getting Common Policy into Vendor Trust Stores was given. Mozilla will not open public discussion on the Common Policy until the FPKIPA provide evidence that FPKI audit requirements are equivalent to WebTrust, ETSI, or ANSI standards.

Ms. Judy Spencer cited a comparison of Audit Standards that was done by Mr. Richard Wilshire in the 2009 timeframe. Ms. Spencer will try to provide a copy to the FPKIMA.

Ms. Spencer also commented that Mozilla and CAB Forum may not fully understand the concept of federated PKIs, which is what the FPKIPA has created through the use of cross-certificate relationships though the FBCA and the Bridge-to-Bridge relationship with CertiPath and SAFE. CertiPath would like to partner with the FPKI if there is an opportunity to educate CAB Forum through some type of presentation. Other organizations who already have a root certificate in Mozilla and are cross-certified with CertiPath have been told they may be removed by Mozilla. Ms. Wendy Brown stated that Mozilla and CAB Forum want to treat cross-certified CAs the same as subordinate CAs because, if a cross-certified CA is compromised due to the potential for a valid path to be built through a bridge, the trust anchor they distribute is just as vulnerable as if the compromised CA was a subordinate. Mozilla and CAB Forum want to limit that risk via technical constraints or by requiring public disclosure of subordinate and affiliate CAs. The FPKI publicly discloses all subordinate and affiliate CAs. A future FPKI TWG discussion on technical constraints is needed.

At the last FPKI TWG meeting, the FPKIMA presented an overview of the plan to provide Enhanced Path Quality Monitoring, including revitalization of the PDVAL test program. The plan was received favorably. The revised PDVAL procedures document will be distributed for FPKI TWG review soon.

The FPKIMA submitted a change proposal for the Common Policy CP to allow the Common Policy CA to be operated as an offline root. There was some resistance to the idea of a longer CRL. The FPKIMA is developing a justification and implementation strategy that will be discussed at the next CPWG meeting.

The FPKI Repositories have been up for over 290 days with no unscheduled break in service. During the latest severe storms, both FPKIMA facilities remained operational. However, the FPKIMA was alerted about network issues at one site around 5:43 AM on Saturday 6/30/2012. Although CRLs were published at 4 am and the other site was able to carry all the traffic, an operational team was deployed to the site to ensure there would be no break in service. It was determined that although the site itself still had power, the ISP to that site had suffered a power outage. The FPKIMA was informed that the Internet Service Provider (ISP) Network Operations Center (NOC) was operating on generator power. The team stayed on site to ensure CRLs were published with no issue at 4:30 pm. At no point was there an interruption to the FPKIMA's ability to provide service to the FPKI Community.

There was a discussion on the repository usage metrics that the FPKIMA provides. Mr. Steve Gregory pointed out that the number of queries shown does not necessarily translate into the number of PKI transactions or certificate validations within the FPKI. Mr. Gregory stated that State has developed a methodology to try to determine transactions vs. repository queries. Mr. Gregory will provide the FPKIMA with the formula State has developed to get a better measurement for the use of State PKI credentials from their repository usage statistics.

ACTION ITEMS:

1. Mr. Steve Gregory to provide information about the model State uses for measurements of PKI usage.

FPKI Certificate Policy Working Group (CPWG) Report, Charles Froehlich

Mr. Charles Froehlich presented the CPWG Report.

a. EKUs and Technical Constraints

CertiPath brought up the idea of a broader implementation of EKUs during a recent joint TWG/CPWG meeting. CertiPath introduced and, the CertiPath Policy Authority approved, a change to their policy that lists optional and restricted EKUs for each of their certificate profiles. CertiPath presented a briefing during the joint session on alternatives for mitigating a vulnerability in the way Microsoft validates signatures on code, which is the driver for their change proposal. There were questions regarding signature validation vulnerability, checking OIDS, and PIV-I cards becoming non-interoperable. The CPWG is assessing risks and benefits of changes resulting from the CertiPath change proposal, and comparing certificate profiles to identify compatibility issues to determine what changes are needed in the FPKI (if any).

b. Discussion: Delegation of Device Sponsor Responsibilities Change Proposal (Common CP)

DHS proposed two change proposals to allow the delegation of device sponsor responsibilities. DHS withdrew the FBCA change proposal after discussions with DoD. The Common Policy CP change proposal allows delegation of sponsor responsibility to an Administrator who has hands-on ability to deal with the device. A final review of this change proposal will be done at the next CPWG meeting.

c. Discussion: Common Root CA Offline Operation

The FPKIMA submitted a change proposal for the Common Policy CP to allow the Common Policy Root CA to be operated offline. Doing so would increase security and improve the ability to respond to disasters. Extensive discussion was held regarding pros/cons and alternatives. The cost of delays and inability to revoke certificates, moving cross-certified CAs, and other related topics were discussed. The CPWG will look into better defining "offline", and defining offline practices and user protections. The CPWG will be polling agencies about how they operate an offline root CA.

d. Other Updates

NIST SP 800-53 Revision 4 (Rev. 4) is now targeted for release in November 2012. It was previously anticipated this month.

The CPWG will be sending an email later this week outlining what is going to be a proposal to work the audit comparisons over the next six months. If NIST SP 800-53 Rev. 4 is not available until November, it’s going to be January 2013 before an updated FPKI security profile (overlay) can be published, assuming most of the changes to controls were accepted (there will be 200 new controls that will need to be evaluated).

Ms. Gallagher will work with DHS to get questions related to the FPKI Overlay included in the FISMA reporting metrics, which should be published in September 2012.

SHA-1 Transition Status, SHA-1 Affiliates

CertiPath mentioned that non-Aerospace and Defense members have shifted to SHA-2, but their other members need to stay in sync with DoD. If necessary, CertiPath will consider options such as a SHA-1 direct trust with DoD, and separating their SHA-1 CAs from FPKI-compliant SHA-2 CAs.

Ms. Mitchell said there is another meeting with the CIO in August 2012 where the SHA-2 transition will be discussed. The end of calendar year 2013 does not work for DoD to transition to SHA-2.

Mr. Gary Wilson said the SAFE-BioPharma Bridge was prepared to move to SHA-2 until they were told this required new CAs per the NIST rule that a CA that issued SHA-1 certificates after 1/1/2011 was not allowed to start issuing SHA-2 certificates. This resulted in a delay to SAFE-BioPharma's plans to move to SHA-2, but they still plan to make the transition this year. However, Mr. Wilson stated that the theoretical risk of attack is not the same as a practical risk, and he feels the actual risk of a SHA-1 collision attack on their members may not be as high as the perceived risk for other targets.

Ms. Brown provided the list of other Affiliates with a SHA-1 relationship to the FPKI. The State of Illinois indicates that they will cross-certify at SHA-2 with the FBCA soon. DEA is SHA-1 only. Symantec/VeriSign have both SHA-1 and SHA-2 CAs.

Ms. Gallagher stated that she has been receiving complaints that some agencies are only accepting ECA certificates for external users (not external PIV-I or SHA-1 credentials). Ms. Gallagher will send these communications to Ms. Mitchell.

ACTION ITEMS:

1. Ms. Gallagher to forward complaints about some agencies not accepting external PIV-I and SHA-1 credentials to Ms. Deb Mitchell.

VA Status Update, John Hancock / Eric Jurasas

No one from the VA was in attendance to provide an update. Ms. Gallagher stated as far as she knows VA has done nothing since they came in and said what they would do in response to their OIG report. Ms. Gallagher has sent notes and talked to people at VA to figure out next steps. Ms. Gallagher may solicit input from the FPKIPA as to next steps

FPKI Chair Update, Deb Gallagher

SLATT meetings are Wednesday mornings. The July ICAMSC is cancelled due to a conflict with the NIST FIPS 201-2 workshop. Everyone is encouraged to attend the NIST workshop.

There will be an IA Symposium in Nashville.

The Attribute Access Control WG (ACAGWG) industry day will be on Sept 5, 2012 to have vendors demonstrate their products capabilities in this space. The ACAGW has established three tiger teams: (1) attribute governance ConOps tiger team; (2) information access policy ConOps tiger team; and (3) level of confidence tiger team.

OMB tasked the FIWG with defining a metric of how successfully an agency is using the approved trusted externally-issued credentials. The accepted metric is the percentage of externally-facing websites accepting the credentials divided by the number of websites requiring logon. This is self reported, but there are tools to verify.

The first NSS IdAM meeting will be on 7/24/12 but then bi-weekly on Thursdays. A gap analysis has been performed between Secret & FICAM fabrics. An implementation plan is now being worked.

The federal cross credentialing tiger team includes agencies such as VA, IRS, CMS, SSA, and the Department of Education. Agencies have not taken up acceptance of externally-issued credentials. They are trying to figure out how to make it easier for agencies to adopt such credentials. The tiger team has developed functional and technical requirements, and use cases, all of which were taken to NSS last week. The proposal was accepted, but the tiger team is still looking at the service model. They were given 30 days to come up with additional details (e.g., cost of each alternative, other issues, proof of concept); then stand up a service model within 120 days. The tiger team is looking to industry to give inputs (maybe an RFI, maybe an industry day). Externally-issued credentials include: Trust Framework Solutions (TFS) third-party credentials (3PC) and PIV-I credentials.

The TFS initiative will be enhanced to include PIV-I. Therefore, TFS will become the central point for all externally-issued credentials.

Many banks are coming forward to be PIV-I providers (VISA will be issuing a smartcard in the next couple of years). Banks work with identity proofing and the "know your customer" rules. Banks may or may not stand up CAs. This is new, so details still need to be looked at (e.g., under what circumstances is face-to-face proofing done).

Government needs to see how to leverage this. A fast-paced progression is likely (e.g., the public will likely next want capability on smartphones). FIPS 201-2 addresses this via Derived Credentials.

There is a lot of interest in PIV-I outside the federal government and outside the US. This may require some FPKI Certificate Policy changes to address PIV-I for foreigners.

HID/ActivitID is no longer cross-certified as a PIV-I issuer as they have severed their relationship with CertiPath. They have moved their CA under VeriSign. Certificates issued by HID prior to June 30, 2012 are still good and will still validate up through the VeriSign relationship. HID is not issuing any new certificates now until they are under the VeriSign infrastructure. HID will become a new PIV-I provider after testing has been completed.

ONC (part of HHS) is asking about PKI. ONC was not originally planning to use PKI, but now they are. Mr. Scott Rea and Ms. Brown answered some of their questions. The FPKIPA will likely be getting many more questions. We need a Frequently Asked Questions (FAQ) document (or something similar) to ensure we give consistent/complete answers and to make getting answers (for all) easy. For example: how does someone cross-certify? We need to look at whether *Crits and Methods* is clear, or if we need to answer any specific questions. Mr. Nathan Faut is working with ONC, representing one state currently wrestling with the new ONC requirements. ONC is requiring health information/insurance exchanges (HIEs) and health information providers (HISP) to use PKI when transmitting healthcare records. ONC is working with the DIRECT Project, which has developed a DirectTrust CP. For those who have not looked at DirectTrust CP, it is less than medium LOA at the federal level. There is a possibility for individual HIEs to apply for cross-certification directly with the FBCA. There will be multiple HIEs per state. When one considers 50 states and 6 territories, that could be a lot of cross-certificates with the FBCA. Some states are looking at a local state-wide bridge that would then cross-certify with the FBCA.

Upcoming meetings and events:

Meeting	Date
Strong Logical Access Tiger Team (SLATT)	**Wednesdays 10:00 – 11:00am**
CPWG & TWG	**July 17, 2012**
FIPS 201 Workshop	**July 25, 2012**
IAB	**August 22, 2012**

Meeting	Date
ISIMSC	**August 2012**
ICAMSC	**August 22, 2012**
IA Symposium (Nashville, TN)	**August 28 – 30, 2012**
ACAG Industry Day	**Sept. 5, 2012**

The next FPKIPA meeting is August 14, 2012. The meeting will not be at USPS. Ms. Gallagher will find a room.

Adjourn Meeting

Ms. Gallagher adjourned the meeting at 11:24 a.m. EST.

FPKIMA Open Action Items

Number	Action Statement	POC	Start Date	Target Date	Status
438	Ms Gallagher will publish the Digital Signature Guidance once a final review is complete; will be published on the web as well.	Deb Gallagher	12-Jul-11	13-Sep-11	Open
460	The FPKIMA will work with Mozilla to determine what Mozilla will accept if we do not provide CPSs	Wendy Brown	8-May-12	30-Jul-12	Open
464	Ms. Darlene Gore to provide the briefing that was given to the BOAC to Mr. Jeff Jarboe for distribution to the FPKIPA.	Darlene Gore, Jeff Jarboe	10-Jul-12	17-Jul-12	Open
465	Mr. Steve Gregory to provide information about the model State uses for measurements of PKI usage.	Steve Gregory	10-Jul-12	17-Jul-12	Open
466	Ms. Gallagher to forward complaints about some agencies not accepting external PIV-I and SHA-1 credentials to Ms. Deb Mitchell.	Deb Gallagher	10-Jul-12	17-Jul-12	Open